REMARKS

Claims 1-14 are pending in the present application. The Official Action rejects Claims 1-14 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,870,474 to Anthony J. Wasilewski, et al. in view of an article by D. Wallner, et al., entitled "Key Management for Multicast: Issues and Architecture" and in further view of U.S. Patent No. 6,880,081 to Yevgeny Itkis. As described below, the rejection of independent Claims 4, 9 and 10 and their respective dependent claims is again traversed, while independent Claims 1, 6, 8 and 11 have been amended to be even further patentably distinct from the cited references. Based on the foregoing amendments and the following remarks, Applicant respectfully requests reconsideration of the present application and allowance of the amended set of claims.

1. The Present Application

As described by the application, a technique is provided for broadcasting secure messages to a plurality of receiving nodes. For example, secure messages may be wirelessly transmitted to each of a plurality of wireless subscribers. The secure messages include data that has been encrypted with a key. The encrypted data and a hashed representation of the key may then be combined into a broadcast message that is transmitted to each of the receiving nodes. In this regard, it is noted that the same broadcast message containing the same encrypted data and the same hashed key, is transmitted to each of the intended recipients.

Upon receiving the broadcast message, each receiving node can parse the broadcast message to separately identify the encrypted data and the hashed key. Each receiving node may also include a plurality of keys that have been prestored in memory, that is, stored by the receiving node prior to receipt of the broadcast message. The receiving node then precedes to hash the plurality of prestored keys. The hashed representations of the prestored keys may be compared to the hashed key included in a broadcast message to determine if a match exists. If a match exists, the encrypted data can be decrypted utilizing the key that has a hash that matches the hashed key included in the broadcast message. If no match exists, the receiving node can request a key from a network entity and, upon receipt of the additional key, can create a hash of the additional key and then compare the hashed representation of the additional key to the hashed key received in the broadcast message to determine if the additional key provided by the network

entity matches that with which the data has been encrypted. If a match is found, the encrypted data is decrypted utilizing the additional key.

By permitting encrypted data to be decrypted by means of a prestored key, the messages may be transmitted with increased security since the key need not be transmitted in a manner that can be deciphered by an unintended recipient. By including a hashed representation of the key in the broadcast message, however, the receiving node can readily determine the key that was used to encrypt the data such that the data may be properly decrypted. Moreover, by utilizing the same key to encrypt the data for each of a plurality of receiving nodes, the same message may be broadcast to and decrypted by each of the intended recipients, thereby conserving network bandwidth and reducing the processing requirements on the transmission side of the network. It is noted that the conservation of bandwidth is of particular concern in instances in which the messages are being wireless transmitted to a plurality of wireless receiving nodes since the wireless network that supports the transmission may have only a limited bandwidth that can be devoted to the transmission of the messages.

As noted, the method of embodiments of the claimed invention is designed to broadcast a secure message to a plurality of receiving nodes, typically while conserving the bandwidth required for the broadcast of the secure message. For various reasons, it is sometimes desirable to prevent one or more of the nodes that previously received and decrypted the secure messages from being capable of decrypting similarly encrypted messages in the future. As described by the application, for example, the receiving nodes may have subscribed to a news service and been provided with the key(s) necessary to decrypt the encrypted news stories that are broadcast to the receiving nodes. Upon the expiration of a node's subscription, however, the receiving node whose subscription has expired should be prevented from decrypting similarly encrypted news stories that are broadcast in the future, while not altering the capability of the other receiving nodes to receive and decrypt any future news stories. In this regard, a message including a NULL key may be transmitted to the node that is desired to be removed from the plurality of receiving nodes. In response to this message, the node to which the NULL key is transmitted replaces the pre-stored keys with the NULL key such that the respective node is thereafter unable to decrypt a broadcast message in the same manner as before. By being capable of transmitting a message containing a NULL key to the node to be removed without

having to retransmit the list of keys to all of the remaining receiving nodes, the bandwidth utilized to administer the broadcast network is further conserved.

2. The Wasilewski '474 Patent

The Wasilewski '474 patent describes a method and apparatus for securely transmitting programs, such as video, audio and data, between a service provider and a customer's set top unit over a broadband digital network. In order to transmit a program, the Wasilewski method and apparatus initially encrypts a program with a first key, such as a random number generated key. The first key is then encrypted with a second key, termed a multisession key (MSK), that is also a randomly generated key. This second key is then encrypted utilizing the public key of the customer's set top unit to which the program is directed. The encrypted program, the encrypted first key and the encrypted second key are then transmitted to the set top unit.

The Wasilewski '474 patent also describes a message authentication code (MAC) and an entitlement management message (EMM) being sent to the set top unit for authentication purposes. In order to generate the MAC and the EMM, hashed representations are created as described below. In one context, control words are delivered to a set top unit along with a message authentication code (MAC). As described in column 9 of the Wasilewski '474 patent, the non-encrypted control word, other data and the MSK are concatenated together and then hashed to produce a MAC. The MAC is appended to an encrypted form of the control word (encrypted with the MSK) and then transmitted to the set top unit along with the resulting hash value. By reversing the process, the message may be authenticated.

The EMM including the MSK may also be transmitted such that the set top unit can confirm that an authorized source transmitted the program and the associated encryption keys. The EMM is hashed and the resulting hash value is encrypted using the private key of the service provider that is to transmit the program content. This encryption process creates a digital signature token that is appended to the EMM. The digitally-signed EMM is then encrypted with the public key of the set top unit that is to receive the message. The signed, encrypted EMM may then also be transmitted to the set top unit.

Upon receipt, the set top unit can decrypt the signed, encrypted EMM with its private key to produce the EMM that includes the MSK and the digital signature token. The token is then

decrypted with the public key of the service provider to result in a hashed representation of the EMM. The EMM that was provided along with the digital signature token is then hashed and the two hashed representations are compared. If equivalent and if the MAC was properly authenticated, the decryption process may continue. In this regard, the decryption of the program may commence by initially decrypting the encrypted second key, i.e., the encrypted MSK, utilizing the private key of the set top unit. The resulting second key is then compared to the MSK that was recovered from the EMM. If the MSKs match, the MSK is considered to be authenticated and the decryption process continues. If the MSKs differ, however, the authenticity of the encrypted program may be in question. If the MSK is authenticated, the encrypted first key may then be decrypted utilizing the MSK. The resulting first key may then be utilized to decrypt the program such that the set top unit can thereafter display the program.

3. Amended Independent Claims 1, 6, 8 and 11 and Their Dependent Claims are Patentable

Amended independent Claims 1, 6, 8 and 11 define a method, a network entity, a computer-readable memory and a computer program product, respectively, for sending secure messages in a broadcast network according to the present invention. With reference to amended independent Claim 1 for purposes of discussion, the method includes the steps of: (i) encrypting data with a key, (ii) hashing the key, (iii) combining the encrypted data and the hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of wireless receiving nodes, (iv) wirelessly transmitting the broadcast message to the plurality of wireless receiving nodes, and (v) removing at least one node from the plurality of wireless receiving nodes by transmitting a message including a NULL key to the node to be removed. As now recited, the message is configured such that the node to be removed replaces the pre-stored key(s) with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key. Independent Claims 6, 8 and 11 have been amended to include comparable recitations albeit in terms of a network entity, a computer-readable memory and a computer program product, respectively.

As described above, prior to receipt of the NULL key, the wireless receiving node had stored one or more keys that the wireless receiving node utilized to decrypt the encrypted data. The message including the NULL key is now recited by independent Claims 1, 6, 8 and 11 to be

configured such that it causes the wireless receiving node to replace the pre-stored key(s) with the NULL key. As a result, the wireless receiving node will thereafter be unable to decrypt messages, at least until the NULL key is replaced by other decryption keys. Thus, the method, network entity, computer-readable memory and computer program product of independent Claims 1, 6, 8 and 11 permit a wireless receiving node to be prevented from successfully decrypting data without having to rekey the other nodes, thereby conserving the bandwidth required to remove the wireless receiving node.

As conceded by the Official Action, "Wasilewski also fails to teach removing at least one node form (sic) the plurality of wireless nodes by transmitting a NULL key to the node to be removed such that the removed node is thereafter unable to decrypt a broadcast message encrypted with said key." However, the Official Action contends that the Itkis '081 patent does describe this feature in column 12, lines 35-67. The Itkis '081 patent describes a method for access control in which a plurality of authorized devices are divided into a plurality of groups. Each of the authorized devices is included in at least one of the groups, but no two authorized devices are included in exactly the same groups. Additionally, a group key is provided to the members of each group such that content that has been encrypted with the group key can be decrypted by members of the group. The Itkis '081 patent also describes a technique for determining the keys known by a device and capable of being utilized by the device to decrypt content. Notably, it is this technique of determining which keys are known by a device that is cited by the Official Action relative to the recitations of independent Claims 1, 6, 8 and 11 relating to the removal of at least one node by transmitting a NULL key to the node to be removed such that the removed node is thereafter unable to decrypt a broadcast message encrypted with a key. However, neither the Itkis '081 patent in general, nor column 12, lines 35-67 of the Itkis '081 patent, more specifically, teach or suggest the general concept of removing a node and, as a result, do not teach or suggest transmitting a message including a NULL key to the node to be removed with the message configured such that the node to be replaced replaces pre-stored key(s) with the NULL key as set forth by independent Claims 1, 6, 8 and 11. Instead, the Itkis '081 patent describes the transmission of encrypted content to a device along with a plurality of encrypted versions of the content key. In this regard, the plurality of encrypted versions are encrypted with various ones of the group keys. In addition, at least one of the

encrypted versions is encrypted with an invalid key, such as a null key. The device then provides decrypted contents and a determination is made as to whether or not the decrypted content is erroneous. Based upon the decrypted content provided by the device, a determination is preferably made as to which one(s), if any, of the group keys are known by the device. For example, in instances in which erroneous content is provided by the device and exactly one invalid or null key was provided to the device, the group key with which the invalid or null key was encrypted is determined to be known to the device such that subsequent content to be securely transmitted to the device can be encrypted in accordance with that same key, i.e., the same key with which the invalid or null key was previously encrypted. See column 13, lines 14-19 of the Itkis '081 patent.

Thus, while the Itkis '081 patent does describe the transmission of an encrypted representation of a null key to a device, the Itkis '081 patent does not teach or suggest the transmission of a message including a null key of the type defined by amended independent Claims 1, 6, 8 and 11. In this regard, the Itkis '081 patent does not teach or suggest the transmission of a message including a NULL key which is configured such that the node to be removed replaces pre-stored key(s) with the NULL key so that the node is thereafter unable to decrypt a broadcast message encrypted with the key(s) that had previously been pre-stored by the node, as set forth by amended independent Claims 1, 6, 8 and 11. In contrast, the invalid or null key transmitted in encrypted form by the Itkis '081 patent is merely intended to determine if the device can recognize and has stored the key with which the invalid or null key is encrypted. If so, the key with which the invalid or null key was encrypted can thereafter be utilized to encrypt content intended for the device since it would be known that the device will recognize the key. As a result, the invalid or null key utilized by the Itkis '081 patent does not cause any key previously stored by the device to be replaced, by the null key or otherwise.

The Wallner article also fails to teach or suggest the removal of a node by the transmission of a message including a NULL key with the message configured such that the node to be removed replaces pre-stored key(s) with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with the pre-stored key(s). Notably, the Official Action does not rely upon the Wallner article for this purpose.

Since none of the references teach or suggest at least the removal of a node by the transmission of a message including a NULL key with the message configured such that the node to be removed replaces pre-stored key(s) with the NULL key so that the removed node is thereafter unable to decrypt a broadcast message encrypted with the pre-stored key(s), amended independent Claims 1, 6, 8 and 11 are also not taught or suggested by any combination of the cited references.

The claims that depend from independent Claims 1, 6, 8 and 11 also are patentably distinct from the cited references for at least the same reasons as described above in conjunction with the amended independent claims. However, some of the dependent claims include additional recitations that provide further bases of patentability. For example, dependent Claim 3 recites that each of the different keys is associated with a respective category of messages. Although the Official Action contends that the association of different keys with respective message categories is described by the Wasilewski '474 patent, it is submitted that the Wasilewski '474 patent does not teach or suggest that the messages are of different categories and, as such, does not teach or suggest the association of different keys with the respective categories. Thus, Applicant submits that the rejection of amended independent Claims 1, 6, 8 and 11, as well as the claims that depend therefrom, is overcome for each of the foregoing reasons.

4. Independent Claim 4 is Patentable

Independent Claim 4 is directed to a method for decrypting a message received over a broadcast network that includes the steps of: (i) receiving data comprising an encrypted message and a hashed key at a node in the broadcast network, (ii) parsing the data to derive the encrypted message and the hashed key, (iii) comparing the received hashed key with a plurality of keys that are prestored at the node and selecting a key having a hash that matches the received hashed key, and (iv) decrypting the encrypted message with the matching key if a match was found. Thus, the method of independent Claim 4 determines which, if any, of a number of prestored keys should be utilized in order to decrypt the encrypted message by hashing the prestored key and comparing the hashed representation of the prestored keys with the hashed key included in the broadcast message.

In contrast, neither the Wasilewski '474 patent nor either of the other cited references teaches or suggests any comparison between a hashed representation of a prestored key and a hashed key included in a broadcast message, as recited by independent Claim 4. Instead, the Wasilewski '474 patent describes the authentication of an encrypted program by creating a hash of an MSK that was transmitted in an encrypted form with another hashed representation of the MSK that was transmitted in hashed format to the set top unit. Thus, the set top unit does not include prestored keys that are hashed and then compared with a hashed key included within a broadcast message. Instead, the Wasilewski '474 patent describes the receipt of a message including both a hashed representation of the MSK and an encrypted, unhashed representation of the MSK and the subsequent comparison of the hashed forms of both MSKs that have been received.

The Official Action indicates that the Wasilewski '474 patent discloses a comparison between a hashed version of a key included in a broadcast message and a prestored key at column 11, lines 24-67. In reviewing the Wasilewski '474 patent including that portion of column 11 highlighted by the Official Action, the set top unit is described to "keep an internal list of public keys corresponding to the private keys of authorized SPs [service providers] **110**." See column 11, lines 46-48. As explained, however, the public keys of authorized service providers do not correspond with the keys that are described to be prestored by independent Claim 4. In this regard, the keys that are prestored in accordance with independent Claim 4 are keys whose hash is compared to a hashed representation of the key that was utilized to encrypt the original message. Thus, as set forth by independent Claim 4, if the hash of one of the prestored keys is found to match the hashed key that is received along with the encrypted message, the prestored key that is found to match the hashed key that is received along with the encrypted message is utilized to decrypt the encrypted message. In contrast, the public keys stored by the set top unit of the Wasilewski '474 patent are utilized to decrypt the digital signature token in order to obtain a hashed representation of the EMM. Thus, the public keys that are stored by the set top unit of the Wasilewski '474 patent are not compared to any other key and, in particular, the hashed representations of the public keys are not compared with a hashed key that is received along with the encrypted message to identify if any one of the public keys matches the hashed key that is received along with the encrypted message, as recited by

independent Claim 4. As such, Applicant therefore submits that the method of independent Claim 4 is not taught or suggested by the Wasilewski '474 patent. In addition, neither of the other cited references teaches or suggests a comparison between a hashed representation of a prestored key and a hashed key included in a broadcast message as set forth by independent Claim 4 and, in fact, neither of the other cited references is cited for any such disclosure. Thus, the rejection of Claim 4, as well as the claims that depend therefrom, is accordingly overcome.

5. Independent Claim 9 is Patentable

Independent Claim 9 describes a computer-readable memory for directing a computer to receive data including an encrypted message and a hashed key, to compare the received hashed key with a plurality of keys and to select a key having a hash matching the received hashed key and to decrypt the encrypted message with the matching key if a match was found and to send a request for a key to a network entity if no matching key was found. In contrast to independent Claim 9, neither the Wasilewski '474 patent nor either of the other cited references teaches or suggests sending a request for a key to a network entity if no matching key was found. The Official Action contends that the Wasilewski '474 patent does request a key from the network entity if a matching key is not found by pointing to column 11, line 48-50. With reference to the internal list of public keys of the authorized service providers that is maintained by the set top unit and was described above, column 11, line 48-50 states "[t]his information is provided to the STU [set top unit] **90** by the conditional access authority to ensure the integrity of the public keys." While the conditional access authority does provide the public keys of the authorized service providers to the set top unit, the Wasilewski '474 patent does not teach or suggest that the conditional access authority provides these public keys in response to a request from the set top unit, let alone a request from the set top unit that is generated in response to having not found any key that matches the hashed key received along with the encrypted message as set forth by independent Claim 9. In addition, neither of the other cited references teaches or suggests sending a request for a key to a network entity if no matching key was found as set forth by independent Claim 9 and, in fact, neither of the other cited references is cited for any such disclosure. As such, Applicant also submits that independent Claim 9 is not taught or suggested

by the cited references, taken either individually or in combination, such that the rejection of Claim 9, as well as Claim 13 that depends therefrom, is overcome.

6. Independent Claim 10 is Patentable

Independent Claim 10 is directed to a computer data signal that includes similar recitations to those described above in conjunction with amended independent Claims 4 and 9. In this regard, independent Claim 10 recites comparing the received hash key with a plurality of keys that are prestored by a receiving node and thereafter decrypting the encrypted message with the matching key if a match was found and, alternatively, sending a request for a key to a network entity if no matching key was found. For each of the reasons described above in conjunction with independent Claims 4 and 9, Applicant submits that none of the cited references, taken either individually or in combination, teaches or suggests independent Claim 10 such that the rejection of Claim 10 is overcome.

7. The Dependent Claims are Patentable

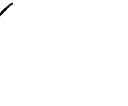
The claims that depend from independent Claims 4 and 9 also are patentably distinct from the cited references for at least the reasons described above in conjunction with independent Claims 4 and 9 such that the rejection of these dependent claims is similarly overcome. However, a number of these dependent claims also include additional recitations that further patentably distinguish the claimed invention from the cited references. In this regard, dependent Claim 5 depends from Claim 4 and further adds the step of requesting a key from a network entity if no prestored key is found to have a hash that matches the received hashed key. As described above in conjunction with independent Claim 9, this additional recitation is not taught or suggested by the cited references, taken either individually or in combination. In addition, Claim 13 depends from independent Claim 9 and recites that the received hashed key is compared with a plurality of keys that have been prestored by the computer. As described above in conjunction with independent Claim 4, the cited references, taken either individually or in combination, also fail to teach or suggest this additional recitation.

CONCLUSION

In view of the amended claims and the remarks presented above, it is respectfully submitted that all of the claims of the present application are in condition for immediate allowance. It is therefore respectfully requested that a notice of allowance be issued. The Examiner is encouraged to contact Applicant's undersigned attorney to resolve any remaining issues in order to expedite examination of the present application

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,



Guy R. Gosnell
Registration No. 34,610

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CLT01/4818714v1